AVVERA SRL SB

NEWSLETTER 2025

# MAGGIO

L'UTILIZZO DELL'INTELLIGENZA ARTIFICIALE NEI PROCEDIMENTI CIVILI: IL CASO CHATGPT WE L'ART. 96 C.P.C.

EHDS: L'UNIONE EUROPEA INAUGURA UNA NUOVA ERA NELLA GESTIONE DEI DATI SANITARI.

IL CASO DEEPSEEK: PROFILI DI GIURISDIZIONE, RESPONSABILITÀ E LIMITI DELL'ENFORCEMENT NEL CONTESTO DIGITALE.

L'AUTORITÀ GARANTE SANZIONA IL TRATTAMENTO DI DATI RELATIVI ALLA GEOLOCALIZZAZIONE DEI LAVORATORI PER FINALITÀ DISCIPLINARI

PROROGA AL 31 LUGLIO SOLO SE VI SONO RICHIESTE DI SUPPORTO

IMQ CERTIFIED QUALITY MANAGEMENT SYSTEM ISO 9001:2015

IMQ CERTIFIED INFORMATION SECURITY MANAGEMENT SYSTEM ISO/IEC 27001:2022

IMQ CERTIFIED OCCUPATIONAL HEALTH AND SAFETY MANAGEMENT SYSTEM ISO 45001:2018

AVVERA | SB Società Benefit

# L'UTILIZZO DELL'INTELLIGENZA ARTIFICIALE NEI PROCEDIMENTI CIVILI: IL CASO CHATGPT E L'ART. 96 C.P.C.

La sezione imprese del Tribunale ordinario di Firenze, con ordinanza emessa il 13 marzo 2025, riflette sul corretto utilizzo degli strumenti di IA nel procedimento giurisdizionale e sull'inquadramento giuridico di comportamenti difensivi privi di valido fondamento giuridico, come nel caso delle cc.dd. **"allucinazioni** "risultato dei sistemi di IA generativa.

Il procedimento trae origine da un reclamo presentato contro il sequestro di merce contraffatta, in cui il reclamante aveva richiesto la condanna della controparte per responsabilità aggravata, sostenendo che quest'ultima avesse riportato, nella propria difesa, estremi di sentenze della Corte di Cassazione risultati del tutto inventati o comunque non coerenti con il contenuto dell'atto; tali riferimenti sarebbero stati inseriti per errore da una collaboratrice dello studio, che avrebbe condotto la ricerca tramite ChatGPT, senza che il patrocinatore in mandato fosse – asseritamente – all'oscuro di tale metodologia.

L'intelligenza artificiale avrebbe generato decisioni apparentemente pertinenti ma in realtà inesistenti, fenomeno noto in letteratura tecnica come *"hallucination",* e confermato dal Collegio stesso per il caso di specie: *"si verifica allorché l'IA inventi risultati inesistenti ma che, anche a seguito di una seconda interrogazione, vengono confermati come veritieri. In questo caso, lo strumento di intelligenza artificiale avrebbe inventato dei numeri asseritamente riferibili a sentenze della Corte di Cassazione inerenti all'aspetto soggettivo dell'acquisto di merce contraffatta il cui contenuto, invece, non ha nulla a che vedere con tale argomento".*

Il Tribunale, pur riconoscendo la gravità dell'omessa verifica e la potenziale pericolosità di un comportamento difensivo fondato su riferimenti giurisprudenziali manifestamente errati, ha tuttavia escluso la sussistenza dei presupposti per l'accoglimento della domanda di condanna per responsabilità aggravata ai sensi dell'art. 96 c.p.c., ritenendo non integrato né il requisito soggettivo della mala fede o della colpa grave previsto dal comma 3, né quello oggettivo del danno, anche solo genericamente allegato, richiesto dal comma 1.

In tale prospettiva, pur stigmatizzando la leggerezza dell'approccio difensivo, il collegio ha concluso per l'inconfigurabilità della responsabilità processuale aggravata, in difetto sia di un comportamento abusivo o strumentale, sia di un pregiudizio concretamente ascrivibile alla condotta censurata.

AVVERA | SB Società Benefit

Infatti, nella motivazione, il Tribunale evidenzia come la parte reclamante non abbia allegato né tantomeno quantificato alcun pregiudizio direttamente ricollegabile all'inserimento delle sentenze inesistenti e come, in ogni caso, la strategia difensiva adottata dalla resistente – incentrata sull'asserita assenza di consapevolezza nella commercializzazione dei prodotti contraffatti – fosse già stata esplicitata nella comparsa di costituzione e risultasse coerente con quanto precedentemente valutato in sede cautelare, rivelandosi pertanto priva di quella connotazione strumentale o mistificatoria necessaria a configurare un abuso del processo. Il collegio ha così escluso l'applicabilità dell'art. 96 c.p.c., riaffermando che tale norma non può essere invocata per sanzionare genericamente errori, omissioni o negligenze difensive, ma solo in presenza di condotte processuali caratterizzate da mala fede manifesta o da una grave scorrettezza incompatibile con la lealtà del contraddittorio.

Al di là dei profili strettamente processuali affrontati nel caso in esame, l'accaduto rileva anche in chiave di data protection in relazione all'AI Act secondo cui sono attribuiti specifici obblighi in capo agli utilizzatori professionali di sistemi di IA (Art 28) imponendo un utilizzo consapevole, informato e tecnicamente sorvegliato delle tecnologie adottate, che in ambito giudiziario, si traduce, in un preciso dovere di diligenza nella comprensione dei limiti strutturali dello strumento impiegato e nella verifica preventiva dell'attendibilità degli output prodotti (tanto più quando vengono impiegati all'interno di atti processuali).

Tali obblighi, appaiono in linea con lo stesso GDPR, che pur non disciplinando direttamente l'uso dell'IA in ambito forense, rimanda ai principi di liceità, correttezza, trasparenza e *accountability*.

In questo contesto, la mancata validazione dei contenuti generati da un sistema di IA, ove utilizzati in un atto giudiziario, non si traduce solo in una scelta metodologica discutibile, ma rischia di costituire una violazione di quei canoni di affidabilità, antropocentrismo e integrità della funzione difensiva che si intendono rafforzare attraverso le normative di settore.

# EHDS: L'UNIONE EUROPEA INAUGURA UNA NUOVA ERA NELLA GESTIONE DEI DATI SANITARI.

L'entrata in vigore del Regolamento (UE) 2025/327 sull'**European Health Data Space (EHDS)**, avvenuta lo scorso 26 marzo, segna un **punto di svolta normativo e operativo** per l'intero ecosistema della salute europea. l'EHDS si afferma come **strumento giuridico vincolante e immediatamente applicabile,** a vantaggio di tutti i cittadini dell'UE, con impatti significativi su sanità pubblica, ricerca, innovazione e governance dei dati all'interno dell'Unione Europea.

La creazione di questo spazio comune rappresenta l'attuazione di uno dei pilastri della strategia europea per i dati, che mira a creare un mercato unico dei dati che garantisca la competitività globale e la sovranità dei dati dell'Europa.

Un doppio binario per i dati: accesso personale e uso pubblico.

Lo spazio europeo dei dati sanitari ha come obiettivo la facilitazione dell'accesso ai dati sanitari e del loro scambio a livello transfrontaliero, al fine di sostenere l'erogazione di assistenza sanitaria e di orientare la ricerca sanitaria e l'elaborazione delle politiche in materia. Il regolamento distingue con chiarezza due grandi ambiti di utilizzo dei dati:

- **Uso primario:** ogni cittadino avrà il pieno diritto di accedere, gratuitamente e in tutta l'UE, ai propri dati sanitari digitali. Dossier clinici, referti, ricette elettroniche, lettere di dimissione: tutto dovrà essere leggibile e interoperabile, garantendo la continuità delle cure anche in contesti transfrontalieri.
- **Uso secondario:** i dati sanitari potranno essere riutilizzati — con rigorose garanzie — per finalità di ricerca scientifica, elaborazione di politiche pubbliche, innovazione medica e sviluppo di intelligenza artificiale. Ma sempre nel rispetto della tutela dei diritti fondamentali e sotto il controllo di autorità nazionali competenti. Resta vietato ogni utilizzo discriminatorio, automatizzato o commerciale (marketing), e viene introdotto un diritto esplicito all'**opt-out** da parte degli interessati, con l'eccezione – regolata – di casi di salute pubblica.

Viene così a configurarsi un delicato equilibrio tra finalità di interesse pubblico e tutela dei diritti fondamentali. Il quadro sarà completato dalle normative nazionali, soprattutto per categorie di dati ad alta sensibilità (genomici, biobanche, applicazioni wellness).

AVVERA | SB Società Benefit

## Chi controlla i dati? Nasce una nuova governance

Il Regolamento stabilisce una serie obblighi e requisiti, destinati a garantire l'efficacia dello Spazio Europeo dei Dati Sanitari.
Inoltre, viene istituito un ecosistema articolato di governance, che si regge su nuove figure chiave:

- **I fornitori di servizi sanitari digitali** (come gli EHR, le app e i sistemi di archiviazione) dovranno garantire l'interoperabilità e la sicurezza dei propri sistemi in conformità con gli standard europei.
- **Gli Health Data Access Bodies (HDAB)** saranno le autorità competenti per valutare le richieste di accesso ai dati per usi secondari. Ogni Stato membro dovrà istituire almeno un HDAB, con il compito di bilanciare l'interesse pubblico con la protezione dei dati personali.
- **I responsabili del trattamento e i fornitori di dati** avranno obblighi più stringenti in termini di qualità, accuratezza, minimizzazione e aggiornamento dei dati trattati.

## Un equilibrio delicato tra innovazione e tutela

L'EHDS crea un nuovo equilibrio tra progresso tecnologico e diritti individuali. Il principio fondamentale è il potenziamento dei diritti dei cittadini riguardo ai propri dati sanitari.

Vengono introdotti nuovi diritti per i pazienti, come l'accesso immediato a determinati dati e la possibilità di condividere informazioni per il trattamento, in ogni parte dell'Unione. Ogni individuo avrà il diritto di accedere, trasferire e gestire i propri dati sanitari elettronici attraverso un portale unico a livello europeo.

L'informazione agli interessati dovrà essere chiara e comprensibile; l'utilizzo secondario sarà subordinato a pseudonimizzazione o anonimizzazione, e i cittadini potranno opporsi all'uso secondario dei propri dati.

Inoltre, i trattamenti dovranno essere soggetti a valutazioni di impatto, soprattutto se basati su tecnologie ad alto rischio, come l'intelligenza artificiale.

## L'infrastruttura tecnica: interoperabilità e qualità dei dati

Uno degli elementi cardine dell'EHDS è la spinta verso un'infrastruttura tecnica comune. Saranno definiti set di dati sanitari europei (European Health Data Sets), modelli di metadati e requisiti di sicurezza per l'interoperabilità tra sistemi nazionali.

A supporto, nasceranno anche **laboratori dati** all'interno delle "fabbriche europee dell'innovazione digitale", con l'obiettivo di raccogliere grandi volumi di dati di alta qualità, curati e sicuri.

Il fascicolo sanitario elettronico (Electronic Health Record – EHR) sarà il fulcro di questo sistema e dovrà rispondere a criteri comuni, per essere utilizzabile in ogni Stato membro. Questo renderà possibile, ad esempio, la lettura di una ricetta elettronica italiana in Germania o la consultazione di un referto francese da parte di un medico in Spagna.

## Sanzioni, controlli e futuro prossimo

Gli Stati membri dovranno designare autorità competenti e prevedere sanzioni effettive in caso di violazione del regolamento. Il sistema è fortemente improntato a un approccio collaborativo, con una governance multilivello che coinvolge Commissione, Stati membri e attori privati.

Con l'EHDS, l'UE non si limita a incentivare l'innovazione: crea un vero e proprio mercato europeo del dato sanitario, accessibile ma sicuro, interoperabile ma regolato.


# IL CASO DEEPSEEK: PROFILI DI GIURISDIZIONE, RESPONSABILITÀ E LIMITI DELL'ENFORCEMENT NEL CONTESTO DIGITALE.

Negli ultimi mesi, *Deepseek* – un modello di AI sviluppato in Cina in grado di eseguire attività allo stesso livello di ChatGPT– ha conquistato l'attenzione per le sue performance sorprendenti. Talmente sorprendenti da sollevare sospetti sulla liceità delle sue modalità di apprendimento, al punto da spingere le autorità europee, incluso il Garante Privacy italiano, ad aprire istruttorie sul trattamento dei dati degli utenti.

Nel gennaio 2025, l'Autorità Garante per la protezione dei dati personali ha emesso un provvedimento con cui ha ordinato alla piattaforma di intelligenza artificiale Deepseek di astenersi dal trattare dati personali riferibili a utenti italiani. Tale misura si fondava sul sospetto che la piattaforma stesse raccogliendo informazioni senza una valida base giuridica, in violazione del Regolamento (UE) 2016/679 (GDPR).

## Quando il diritto incontra i limiti del digitale.

Nonostante l'ordine impartito a gennaio 2025, Deepseek risulta ancora raggiungibile dall'Italia, pertanto, l'Autorità Garante dei dati personali è tornata sulla questione, ma lo ha fatto in modo inusuale: trasmettendo una PEC ai principali operatori di connettività italiani, allegando copia del provvedimento e "invitando" gli stessi ad adottare "ogni determinazione di competenza" per impedire l'accesso al servizio da parte degli utenti nazionali.
Una scelta che solleva rilevanti profili di legittimità giuridica, efficacia amministrativa e coerenza sistematica nel delicato equilibrio tra tutela dei diritti fondamentali e limiti dell'azione regolatoria nel cyberspazio.

## Profili critici dell'intervento del Garante.

**Assenza di un ordine formale vincolante**
L'atto trasmesso ai provider non costituisce un provvedimento esecutivo ai sensi della normativa amministrativa italiana. L'espressione "ogni determinazione di competenza", priva di contenuto precettivo chiaro, non impone alcuna misura concreta, configurandosi più come un atto di moral suasion che come un obbligo giuridico.

**Incapacità tecnica e giuridica degli operatori di rete**
I fornitori di accesso a Internet non dispongono, in assenza di uno specifico ordine dell'autorità giudiziaria o amministrativa, del potere di bloccare selettivamente l'accesso a determinati contenuti. La violazione è prevista dall'art. 15 della Costituzione, che tutela la libertà e la segretezza delle comunicazioni. Interventi sul traffico dati — ad esempio tramite DNS hijacking o IP blocking — sono legittimi solo se previsti espressamente da provvedimenti motivati.

**Limiti di giurisdizione**
La piattaforma Deepseek non ha una stabile organizzazione in Italia, non è localizzata in lingua italiana, e non è rivolta specificamente al mercato nazionale. Di conseguenza, non è scontato che possa ritenersi soggetta alla giurisdizione italiana, secondo i criteri previsti dal GDPR (art. 3) o dal diritto penale nazionale (art. 6 c.p.).

## La non applicabilità del Digital Services Act

Alcuni commentatori hanno richiamato l'articolo 7 del Digital Services Act (Reg. UE 2022/2065), che consente agli intermediari di adottare misure volontarie per garantire il rispetto delle leggi. Tuttavia, tale facoltà non può derogare ai principi costituzionali italiani: l'intercettazione e la limitazione delle comunicazioni sono ammissibili solo in presenza di un atto autorizzativo emanato da un'autorità competente.

L'art. 9 DSA, che disciplina la rimozione di contenuti illegali, non è pertinente nel caso di specie, in quanto non si tratta di contenuti ma di operazioni di trattamento dati.

## Una riflessione sul modello regolatorio

L'approccio adottato dal Garante solleva interrogativi più ampi circa il modello di enforcement che si sta progressivamente affermando nel contesto digitale. Il trasferimento, implicito o esplicito, del potere decisionale verso soggetti privati — provider, piattaforme, content moderator — rischia di generare un sistema di **regolazione "paralegale"**, che sfugge ai meccanismi tradizionali di responsabilità, garanzia e controllo democratico.

In tale contesto, si assiste alla trasformazione della norma giuridica in semplice indicazione comportamentale, e del provvedimento amministrativo in suggerimento non vincolante. Un'evoluzione che, se non bilanciata da un solido impianto di legittimità, mette a rischio **i principi dello Stato di diritto nel contesto della governance digitale.**

## Conclusioni

Il caso Deepseek rappresenta un esempio paradigmatico delle difficoltà che le autorità nazionali incontrano nel garantire l'effettività delle norme a tutela dei dati personali, quando i soggetti coinvolti operano al di fuori della loro giurisdizione e delle strutture istituzionali europee.

La risposta, tuttavia, non può consistere in soluzioni ambigue o scorciatoie regolatorie. Al contrario, è necessario rafforzare i canali di cooperazione internazionale, chiarire i presupposti di giurisdizione extraterritoriale e preservare il ruolo centrale dell'autorità giudiziaria nei procedimenti che incidono su diritti fondamentali.

# L'AUTORITÀ GARANTE SANZIONA IL TRATTAMENTO DI DATI RELATIVI ALLA GEOLOCALIZZAZIONE DEI LAVORATORI PER FINALITÀ DISCIPLINARI

L'Autorità Garante si è recentemente espressa relativamente al trattamento dei dati di geolocalizzazione dei dipendenti, nell'ambito del rapporto di lavoro svolto in modalità agile, per finalità disciplinari (Provvedimento n. 10128005 del 13 marzo 2025).

Nel caso in esame, la dipendente ha lamentato l'illegittimo trattamento dei propri dati personali da parte del datore di lavoro, in quanto finalizzato a verificare la corrispondenza tra il luogo di svolgimento della prestazione lavorativa e quanto indicato nell'accordo in materia di lavoro agile sottoscritto con la società.

Dall'istruttoria svolta dal Garante è emerso che tali controlli erano svolti, nell'ambito di puntuali attività di verifica, con le seguenti modalità: il responsabile dell'Ufficio aziendale preposto contattava il lavoratore (scelto su base casuale) e domandava, nel rispetto della fascia oraria di reperibilità, una timbratura tramite l'applicativo *"Time relax"*, previo consenso del lavoratore alla geolocalizzazione. Successivamente, il dipendente era invitato a inviare una mail al Responsabile dell'Ufficio aziendale incaricato del controllo, indicando il luogo di svolgimento della prestazione lavorativa, in modo da consentire al Responsabile preposto di verificare la corrispondenza tra quanto dichiarato dal dipendente nella mail e quanto rilevato dal sistema di geolocalizzazione.

Il Garante ha ribadito che il datore di lavoro può trattare dati personali dei lavoratori (anche particolari) solo in presenza di un'idonea base giuridica, ossia se: (i) il trattamento è necessario per la gestione del rapporto di lavoro, (ii) per adempiere a specifici obblighi derivanti dalla disciplina di settore, o (iii) quando il trattamento è "necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" (nell'ambito di una prestazione lavorativa in ambito pubblico).

Sotto il profilo dei controlli l'Autorità ha evidenziato come eventuali verifiche, tramite l'impiego di strumenti tecnologici, da quali derivi anche la possibilità di un controllo a distanza dei lavoratori possano svolgersi solo nel rispetto di quanto prescritto dalla normativa di settore (art. 4. comma 1, della L. n. 300 del 1970, c.d. Statuto dei lavoratori), ossia per "esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale", previo accordo con le rappresentanze sindacali e dopo aver fornito al lavoratore informazioni adeguate in merito alle modalità d'uso degli strumenti e di effettuazione dei controlli.

Ciò premesso, l'Autorità ha ritenuto che eventuali controlli in merito all'osservanza dei doveri di diligenza da parte del lavoratore, rientrino nelle prerogative del datore di lavoro solo se svolti personalmente dal datore di lavoro o attraverso la propria organizzazione gerarchica e non possano, al contrario, essere svolti con strumenti tecnologici a distanza, che ridurrebbero lo spazio di libertà e dignità della persona, comportando un monitoraggio diretto dell'attività del lavoratore non consentito dall'ordinamento vigente.

Tale finalità di trattamento non risulta, infatti, riconducibile ad alcuna delle finalità disciplinate dal legislatore *("organizzative e produttive", "di sicurezza del lavoro" e "di tutela del patrimonio aziendale")*, atteso che il controllo a distanza dell'attività lavorativa è consentito dalla legge, nel rispetto delle condizioni di garanzia ivi previste, solo incidentalmente, ossia in occasione del perseguimento di tali legittime finalità, così assumendo un carattere tipicamente indiretto.

Nel corso del procedimento, l'Autorità Garante ha, inoltre, rilevato l'inadeguatezza delle informazioni fornite ai lavoratori sul trattamento dei propri dati personali (art. 13 del Regolamento) e il mancato svolgimento di una valutazione d'impatto del trattamento dei dati relativi alla geolocalizzazione del personale dipendente in modalità agile (art. 35 del Regolamento).

Per quanto sopra esposto, l'Autorità Garante rilevata l'illiceità del trattamento ha ingiunto alla società il pagamento di una sanzione amministrativa di euro 50.000,00.

# PROROGA AL 31 LUGLIO SOLO SE VI SONO RICHIESTE DI SUPPORTO

L'Agenzia per la cybersicurezza nazionale ha comunicato che il termine ultimo entro cui completare le attività di aggiornamento annuale delle informazioni **da parte dei SOLI soggetti NIS che hanno bisogno di svolgere maggiori approfondimenti** è posticipato al 31 luglio p.v..

Tale slittamento è stato deciso in considerazione dell'alto numero di richieste di assistenza in corso ed è stato comunicato con una news del 23 maggio.

Stando ai numeri resi pubblici dall'Agenzia per la cybersicurezza nazionale nella comunicazione dello scorso 15 aprile, l'elenco dei soggetti NIS conta oltre **20.000 organizzazioni**, di cui oltre **5.000 con la qualifica di soggetti essenziali.** Come noto la seconda fase consiste in una serie di adempimenti in capo ai soggetti NIS relativi alla conferma, aggiornamento o integrazione delle informazioni inizialmente fornite. Si tratta di informazioni utili a inquadrare il soggetto NIS, i suoi operatori, i suoi contatti, il suo perimetro di operatività e, non ultima, l'individuazione dei soggetti responsabili delle violazioni. A una settimana dalla scadenza entro cui deve essere completata questa seconda fase, Risulta che:

- circa **la metà dei soggetti NIS ha inserito una parte delle informazioni richieste, e**
- **oltre mille hanno terminato l'aggiornamento.**

I numeri riportati dimostrano presumibilmente un certo affanno delle organizzazioni in perimetro, specie di quelle che hanno aperto un ticket, e questo ha portato l'Agenzia a un intervento che andasse nel solco del percorso di ascolto e collaborazione già attivato nei mesi precedenti.

In estrema sintesi quindi **i soggetti NIS che hanno richiesto supporto per la finalizzazione dell'aggiornamento annuale dei dati potranno concludere tale procedura entro il 31 luglio.**

Nell'ambito della stessa news del 23 maggio l'Agenzia per la cybersicurezza nazionale ha infine informato che la presa d'atto telematica da parte dei membri degli organi amministrativi e direttivi potrà essere effettuata anche successivamente al termine del 31 luglio. Questo significa che il soggetto NIS sarà ottemperante una volta che il punto di contatto ha censito i suddetti soggetti, anche in assenza della conseguente formale "accettazione" (che ricordiamo è possibile solo con un accesso al portale servizi da parte dei singoli soggetti effettuato con SPID o credenziali).

AVVERA | SB Società Benefit

AVVERA | SB Società Benefit

## SEDE LEGALE E OPERATIVA
20146 MILANO
VIA SARDEGNA, 21

## SEDE OPERATIVA CERTIFICATA
21040 ORIGGIO (VA)
LARGO UMBERTO BOCCIONI, 1

## ALTRE SEDI
61211 PESARO (PU)
VIA GIASONE DEL MAINO, 13
33100 UDINE (UD)
VIA G. TULLIO, 22

## TELEFONO
+39 0296515401

## FAX
0296515499

## C.F./P.IVA 06047090961
## CAP. SOC. 300.000 EURO I.V.
REG. IMPO. MI
06047090961
REA 1866500

## WWW.AVVERA.IT
## AVVERA@LEGALMAIL.IT

IMQ CERTIFIED
QUALITY MANAGEMENT SYSTEM
ISO 9001:2015

IMQ CERTIFIED
INFORMATION SECURITY MANAGEMENT SYSTEM
ISO/IEC 27001:2022

IMQ CERTIFIED
OCCUPATIONAL HEALTH AND SAFETY MANAGEMENT SYSTEM
ISO 45001:2018